

Games with Opacity Condition

Bastien Maubert and Sophie Pinchinat
IRISA, France

Abstract. We describe the class of games with opacity condition, as an adequate model for security aspects of computing systems. We study their theoretical properties, relate them to reachability perfect information games and exploit this relation to discuss a search approach with heuristics, based on the directing-word problem in automata theory.

1 Introduction

We describe a class of two-player imperfect information games that we call *games with opacity condition*. In these games, the players are Robert (for “robber”) and Gerald (for “guardian”). Imperfect information is asymmetric between the players: Robert has imperfect information as opposed to Gerald who has perfect information. The model we used for games with opacity condition uses the classic imperfect information arenas, as defined in [12, 4, 1], but it differs in the nature of the winning objectives: in games with opacity, Gerald aims at maintaining the uncertainty of Robert regarding the actual position in the game along the play.

Games with opacity conditions easily relate to computer systems security issues, since in practice interactive systems are expected to have a policy against intruders that attempt to reach a secret, modelled e.g as perfect information in the model.

Our claim that games with opacity condition are natural and adequate models for practical applications is all the more sustained by very recent contributions of the literature [13, 5]. These results mainly arise from the analysis of discrete-event systems and their theory of control. We believe that the abstract setting provided by the game-theoretical paradigm enables to focus on essential aspects such as circumventing the complexity of the problems and synthesizing strategies.

In this contribution, we first establish that deciding the opacity-guarantee problem translates into the problem of solving a perfect information safety game – which, according to determinacy in the perfect information setting, is dual to a perfect information reachability game. This is a key point of our approach: although standard bottom-up techniques to solve safety perfect information games are intractable in this case, due to a blow-up in the translation, top-down methods may be worth considering. Moreover, these methods may be enriched with heuristics, preventing the search from a useless exhaustive exploration of the entire state space.

We therefore discuss a search-based approach in an AND/OR graph (the perfect information arena of a reachability game). The search is sustained by heuristics arising from a standard problem in automata theory: the *directing-word problem* [3, 10], which addresses the existence of a finite word that leads every state of a non-deterministic automaton to a unique single state; the literature also refers to the *synchronizing word* or the *reset* problem.

The paper is organized as follows. In Section 2 we introduce the model and the notion of opacity, and we define the opacity-guarantee and opacity-violate problems. Theoretical analysis of games with opacity condition is done in Section 3, where their non-determinacy is proved, and the equivalence of the opacity-guarantee and opacity-violate problems with a safety, respectively reachability perfect information game is established as well as their connection with the directing-word problem. Finally, we end by Section 4 where we discuss a search approach with heuristics based on directing-word techniques.

2 Games with opacity condition

2.1 Arena, strategies

An *imperfect-information arena* over the alphabet Σ and the set of observations Γ is a structure $A = (V, \Delta, \text{obs}, \text{act})$ where V is a finite set of *positions*, $\Delta : V \times \Sigma \rightarrow 2^V$ is a transition function, $\text{obs} : V \rightarrow \Gamma$ is an observation function and $\text{act} : \Gamma \rightarrow 2^\Sigma \setminus \{\emptyset\}$ assigns

to each observation the non-empty set of available actions. The fact that act is defined on Γ reflects the fact that available actions must be identical for observationally equivalent positions.

We sometimes write γ instead of $\text{obs}^{-1}(\gamma)$ to denote the set of positions $v \in V$ whose observation is γ .

In an arena $A = (V, \Delta, \text{obs}, \text{act})$, the players Robert and Gerald play as follows.

First, before the game starts, Gerald chooses an initial position v_0 . We refer to the game A just after v_0 has been chosen in the first round by A_{v_0} . Then Robert chooses an action $a_1 \in \text{act}(v_0)$, and Gerald chooses a position $v_1 \in \Delta(v_0, a_1)$. In the next round, we proceed similarly but from position v_1 where Robert is given the information $\text{obs}(v_1)$ to choose a suitable action $a_2 \in \Sigma$. A *concrete play* in A_{v_0} is an infinite sequence $\rho = v_0 a_1 v_1 a_2 v_2 a_3 \dots \in v_0(\Sigma V)^\omega$ that results from an interaction of Robert and Gerald in this game.

We now extend obs as a morphism $\text{obs} : (V \cup \Sigma)^* \rightarrow (\Gamma \cup \Sigma)^*$, by letting $\text{obs}(a) = a$, for all $a \in \Sigma$. The imperfect information setting leads Robert to partially observe a concrete play ρ as the *abstract play* $\text{obs}(\rho) \in \gamma_0(\Sigma \Gamma)^\omega$, where $\gamma_0 := \text{obs}(v_0)$.

Since Gerald has perfect information on how the play progresses, a strategy of Gerald in A_{v_0} is a mapping of the form

$$\beta : v_0(\Sigma V)^* \Sigma \rightarrow V$$

On the contrary, because the information revealed to Robert is based on observations, a strategy of Robert in A_{v_0} is a mapping of the form

$$\alpha : \gamma_0(\Sigma \Gamma)^* \rightarrow \Sigma$$

For every natural number $k \in \mathbb{N}$, we denote by $\pi^k \in \gamma_0(\Sigma \Gamma)^k$ the k -th prefix of π , defined by $\pi^k := \gamma_0 a_1 \gamma_1 a_2 \gamma_2 \dots a_k \gamma_k$, with the convention that $\pi^0 = \gamma_0$. We denote by π^+ an arbitrary prefix of π , and we may use analogous notations for concrete plays.

Given strategies α and β of Robert and of Gerald respectively, we say that a play $\rho = v_0 a_1 v_1 \dots$ is *induced by* α if $\forall i \geq 1, a_i = \alpha(\text{obs}(\rho^{i-1}))$, and ρ is *induced by* β if $\forall i \geq 1, v_i = \beta(\rho^{i-1} a_i)$.

2.2 Opacity condition

Let us fix an abstract play $\pi = \gamma_0 a_1 \gamma_1 a_2 \gamma_2 \dots$. Note that every k -th prefix of π characterizes a unique *information set* $I(\pi^k) \subseteq V$ consisting of the set of plausible actual concrete positions of Robert in the game after k rounds. Formally, $I(\pi^0) := \gamma_0$, and $I(\pi^{k+1}) := \Delta(I(\pi^k), a_{k+1}) \cap \gamma_{k+1}$, for $k \in \mathbb{N}$. For a concrete play ρ we define $I(\rho^k) := I(\text{obs}(\rho^k))$.

A (concrete) play ρ satisfies *the opacity property*, or is *opaque*, if for every natural number k , $I(\rho^k)$ is not a singleton, that is $|I(\rho^k)|^1$ is strictly greater than 1.

Informally, the opacity condition means that the actual position along the play is never revealed to Robert.

We investigate effective methods to solve *games with opacity condition*, that is to answer the following *opacity-guarantee problem*: *Given an imperfect-information arena $A = (V, \Delta, \text{obs}, \text{act})$ and an initial position v_0 , does Gerald have a strategy β in A_{v_0} such that any play induced by β is opaque?*

Actually, driven by the natural application domains underlying this game-theoretic problem, we also expect to compute a winning strategy for Gerald, when it exists. We also define the *opacity-violate problem*, dual to the opacity-guarantee problem, that consists in deciding the existence of a strategy α for Robert such that no play induced by α is opaque. If the answer to the opacity-guarantee problem is positive, v_0 is a *winning position* for Gerald. Similarly, if the answer to opacity-violate problem is positive, then v_0 is a winning position for Robert.

3 Results on games with opacity condition

We first establish the non-determinacy of games with opacity condition. We next show how the opacity-guarantee and the opacity-violate problems can be rephrased in terms of solving a safety perfect information game and a reachability perfect information game

¹ the cardinal of $I(\rho^k)$.

respectively. Finally we introduce the *directing-word problem* and show a polynomial time reduction to the opacity-violate problem. From the above, we end the section by inferring complexity results.

3.1 Non-determinacy

We recall that a game is *determined* if each position is winning for one player or the other. It is well known that perfect-information games are determined [9], and that imperfect-information games are not determined in general. We prove the following:

Theorem 1. *Games with opacity condition are not determined in general.*

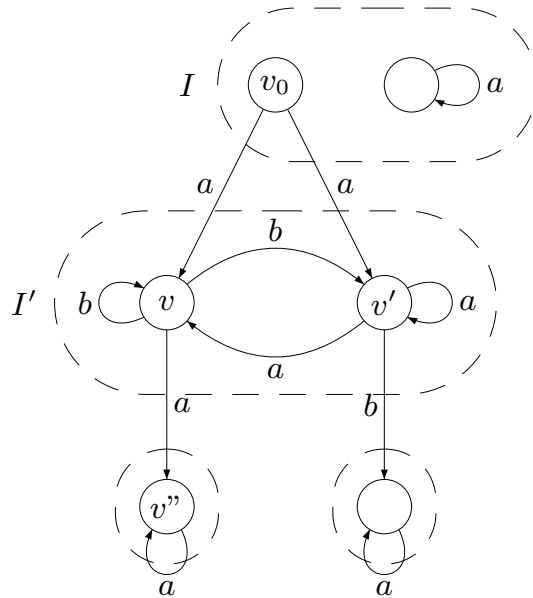


Fig. 1. A game with opacity condition

Proof. Consider the game on Figure 1. Note that the dashed sets represent observation classes. We first prove that Robert does not have a winning strategy in the initial position v_0 .

Robert has information set I , and he must play a . Next Gerald chooses one of the two reachable positions v and v' and Robert now

knows the information set I' . There are two possibilities: Robert can either play a or b . If he plays a , then if the actual position is v , Robert wins (he reaches v'' that is alone in its observation class). But if the actual position is v' , then Gerald can whether choose to loop, whether move to v . Notice that in both cases, Robert still knows information set I' : he never gains information, thus can never know if he should play a or b . Then the strategy of playing a at the second round is not winning. Reversing the roles of a and b in this reasoning yields the result that playing b at the second round is not winning neither. Robert does not have a winning strategy.

We now prove that Gerald does not have a winning strategy either. As we said, at first Robert can only choose a . If Gerald chooses v , then Robert can win by playing a , and if he chooses v' , Robert can win by playing b . So there is no winning strategy for Gerald neither. \square

3.2 Reductions to perfect information games

We informally describe a powerset construction that leads to solve an alternating reachability problem in a perfect information game. This construction is strongly inspired from the one of [12].

Let $A = (V, \Delta, \text{obs}, \text{act})$ be an imperfect-information arena, and v_0 be the initial position chosen by Gerald. We define a two-player perfect information arena \tilde{A}_{v_0} , where the players are Roberta and SuperGeraldine².

A position of \tilde{A}_{v_0} is either I where I is a reachable information set in the game A_{v_0} – it is a position of Roberta –, or (I, a) where I is a reachable information set in A_{v_0} , and $a \in \text{act}(I)$ – it is a position of SuperGeraldine.

The game is played as follows. It starts in the initial position $I_0 := \text{obs}(v_0)$ of Roberta. In a position I , Roberta chooses $a \in \text{act}(I)$ and moves to position (I, a) . Next, define O the set of reachable

² We use the superlative “Super” here because in general the winning strategies of SuperGeraldine do not reflect any winning strategy of Gerald in A_{v_0} . She has “more power” than Gerald.

observations from I by a : let Π_I denote the set of prefix plays ρ^+ in A_{v_0} such that $I(\rho^+) = I$. Now pose $O := \{\text{obs}(v') \mid v' \in \Delta(v, a), v = \text{last}(\rho^+), \rho^+ \in \Pi_I\}$. SuperGeraldine chooses a non empty information set $\Delta(I, a) \cap \gamma$, where γ ranges over O . In \tilde{A}_{v_0} , a play $I_0(I_0, a_1)I_1(I_1, a_2) \dots$ is winning for Roberta if it reaches a position of the form $\{v\}$, otherwise it is winning for SuperGeraldine.

Theorem 2. *Robert has a winning strategy in A_{v_0} , if and only if, Roberta has a winning strategy in the perfect information game \tilde{A}_{v_0} .*

Theorem 2 has been proved by Reif in [12]. He establishes a 1–1 correspondence between winning strategies in A_{v_0} and winning memoryless strategies in \tilde{A}_{v_0} . However since our model, though equivalent to his, looks different, we explicate the correspondence between strategies in our model, but do not provide its proof of correctness as it exactly matches the one in [12, page 288]:

- Let α be a winning strategy of Robert. Define the memoryless strategy $\tilde{\alpha}$ of Roberta by $\tilde{\alpha}(I) := (I, \alpha(\text{obs}(\rho^+))$, for some prefix concrete play ρ^+ in the game A_{v_0} such that $I(\rho^+) = I$.
- Let $\tilde{\alpha}$ be a memoryless winning strategy of Roberta in \tilde{A}_{v_0} . Define the strategy α of Robert in A_{v_0} by: for any prefix abstract play π^+ , $\alpha(\pi^+) := a$, with $(I(\pi^+), a) = \tilde{\alpha}(I(\pi^+))$.

We now establish Theorem 3 demonstrating a powerset construction for Gerald, leading to a safety perfect information game \hat{A}_{v_0} . In this game, we maintain an extra information on how Gerald is playing in A_{v_0} . The players in \hat{A}_{v_0} are SuperRoberta³ and Geraldine. A position in \hat{A}_{v_0} is either of the form (I, v) where I is a reachable information set in A_{v_0} , and $v \in I$ – it is a position of SuperRoberta –, or of the form (I, v, a) where I is a reachable information set in A_{v_0} , $v \in I$, and $a \in \text{act}(v)$ – it is a position of Geraldine. The initial position is $(\text{obs}(v_0), v_0)$. In position (I, v) , SuperRoberta chooses $a \in \text{act}(v)$, and moves to (I, v, a) . In position (I, v, a) , Geraldine chooses $v' \in \Delta(v, a)$ and moves to (I', v') where

³ we use the superlative “Super” as, contrary to what Roberta could do in the game \tilde{A}_{v_0} , SuperRoberta can take advantage of the extra information.

$I' = \Delta(I, a) \cap \text{obs}(v')$. In \widehat{A}_{v_0} , a play $(I_0, v_0)(I_0, v_0, a_1)(I_1, v_1) \dots$ is winning for SuperRoberta if it reaches a position (I, v) or (I, v, a) where $|I| = 1$, otherwise it is winning for Geraldine.

Theorem 3. *Gerald has a winning strategy in A_{v_0} , if and only if, Geraldine has a winning strategy in the perfect information game \widehat{A}_{v_0} .*

Proof. We establish a 1–1 correspondence between winning strategies in A_{v_0} and winning memoryless strategies in \widehat{A}_{v_0} .

- Let β be a winning strategy of Gerald. Define the strategy $\widehat{\beta}$ of Geraldine by

$$\widehat{\beta}((I_0, v_0)(I_0, v_0, a_1)(I_1, v_1) \dots (I_n, v_n, a_{n+1})) := (I_{n+1}, v_{n+1})$$

with $v_{n+1} = \beta(v_0 a_1 v_1 \dots v_n a_{n+1})$ and $I_{n+1} = \Delta(I_n, a_{n+1}) \cap \text{obs}(v_{n+1})$. We prove by contradiction that $\widehat{\beta}$ is winning for Geraldine in \widehat{A}_{v_0} . Assume $\widehat{\beta}$ is not winning, we show that β is not winning for Gerald in A_{v_0} . There exists $\widehat{\rho}^n = (I_0, v_0)(I_0, v_0, a_1) \dots (I_n, v_n)$ a prefix of a play $\widehat{\rho}$ in \widehat{A}_{v_0} induced by $\widehat{\beta}$ such that $|I_n| = 1$. From the definition of $\widehat{\beta}$ we have that $\rho^n = v_0 a_1 v_1 \dots v_n$ is a prefix of a play in A_{v_0} induced by β . We show that this prefix is losing for Gerald by proving that $\forall i \leq n, I(\rho^i) = I_i$. We proceed by induction over i : clearly $I(\rho^0) = \text{obs}(v_0) = I_0$. Suppose $I(\rho^i) = I_i$, for $0 \leq i < n$.

$$\begin{aligned} I(\rho^{i+1}) &= \Delta(I(\rho^i), a_{i+1}) \cap \text{obs}(v_{i+1}) \\ &= \Delta(I_i, a_{i+1}) \cap \text{obs}(v_{i+1}) \\ &= I_{i+1} \end{aligned}$$

So $|I(\rho^n)| = |I_n| = 1$, and β is not winning. By contradiction, $\widehat{\beta}$ is winning.

- Let $\widehat{\beta}$ be a winning strategy of Geraldine. For a prefix $\rho^n = v_0 a_1 v_1 \dots v_n$ and an action $a_{n+1} \in \text{act}(v_n)$, we define the strategy β of Gerald by $\beta(\rho^n a_{n+1}) := v_{n+1}$ with $(I_{n+1}, v_{n+1}) = \widehat{\beta}((I(\rho^0), v_0)(I(\rho^0), v_0, a_1) \dots (I(\rho^n), v_n, a_{n+1}))$. We prove again by contradiction that β is winning for Gerald in A_{v_0} .

Assume β is not winning. There exists a prefix $\rho^n = v_0 a_1 v_1 \dots v_n$ of a play ρ induced by β such that $|I(\rho^n)| = 1$.

Let $\widehat{\rho} = (I(\rho^0), v_0)(I(\rho^0), v_0, a_1) \dots (I(\rho^n), v_n)$. It is a prefix of a play in \widehat{A}_{v_0} that is losing for Gerald. We need to prove that it is induced by $\widehat{\beta}$. For $i < n$, let I_{i+1} be the information set such that $\widehat{\beta}((I(\rho^0), v_0)(I(\rho^0), v_0, a_1) \dots (I(\rho^i), v_i)) = (I_{i+1}, v_{i+1})$.

$$\begin{aligned} I_{i+1} &= \Delta(I(\rho^i), a_{i+1}) \cap \text{obs}(v_{i+1}) \text{ from the construction of } \widehat{A}_{v_0} \\ &= I(\rho^{i+1}) \text{ by definition of } I \end{aligned}$$

$\widehat{\rho}^n$ is induced by $\widehat{\beta}$ and is losing for Gerald, so $\widehat{\beta}$ is losing. Contradiction. \square

3.3 The directing-word problem

We define the directing-word problem, a classic problem in automata theory originally considered in [11, 3].

Given a non-deterministic complete finite-state automaton $\mathcal{A} = (Q, X, \delta)$ over alphabet X , a *directing word* in \mathcal{A} is some $w \in X^*$ such that $|\delta(Q, w)| = 1$.

The *directing-word problem* is a decision problem: *Given a non-deterministic complete finite-state automaton \mathcal{A} , does there exist a directing-word in \mathcal{A} ?*

Proposition 1. *The directing-word problem is in PSPACE.*

Proof. Not surprisingly, a powerset construction and a guess on how a subset of the form $\{q\}$ is reachable from the full subset Q , shows a solution of the problem in NPSPACE, which equals PSPACE by the Theorem of Savitch [14]. \square

However, we are not aware whether the directing-word problem is PSPACE-hard or not. Under the hypothesis that the automata are deterministic, the problem, known as the *synchronizing word problem* [2] has been extensively studied. In particular, it is NP-complete to decide whether there exists a synchronizing word of length $\leq k$, and

the Cerny conjecture states that if a synchronizing word exists, then so does a synchronizing word of length at most $(n - 1)^2$ [10, 2]. In the general case, the powerset construction in Proposition 1 shows an exponential bound on the length of a minimal directing word [6].

We establish a polynomial reduction of the directing-word problem into the opacity-violate problem. Let $\mathcal{A} = (Q, X, \delta)$ be a non-deterministic complete finite-state automaton. We construct the arena $A^{\mathcal{A}} = (Q, \delta, \text{obs}, \text{act})$ over X and $\{\gamma\}$ (a fresh symbol), such that Proposition 2 holds. Let $\text{act}(v) = X$, for every v , since \mathcal{A} is complete, and obs be the constant mapping sending any position to the unique observation γ ; notice that Robert is consequently blindfold – in the sense of [12]. Let v_0 be any position in Q .

Proposition 2. *Robert wins the game $A_{v_0}^{\mathcal{A}}$ if, and only if, there exists a directing word in \mathcal{A} .*

Proof. Assume there exists a directing word $w = x_1x_2 \dots x_\ell$ in \mathcal{A} of length ℓ , which leads any state of \mathcal{A} to the state q_w . We use w to define the winning strategy α_w of Robert in the game $A_{v_0}^{\mathcal{A}}$ as:

$$\begin{cases} \alpha_w(\gamma x_1 \gamma x_2 \dots \gamma x_i \gamma) := x_{i+1}, & \text{for all } 0 \leq i < \ell, \\ \alpha_w(\gamma x_1 \gamma x_2 \dots (x_\ell \gamma)^k) := x_\ell, & \text{for all } k > 0. \end{cases}$$

Reciprocally, assume there exists a winning strategy α for Robert in $A_{v_0}^{\mathcal{A}}$. Since there is only one observation, the only possible abstract play induced by this strategy is $\pi = \gamma \alpha(\gamma) \gamma \alpha(\gamma \alpha(\gamma) \gamma) \dots$. Projecting the least prefix π^+ of π such that $|I(\pi^+)| = 1$ on X gives a directing word for \mathcal{A} . \square

3.4 On the complexity of opacity problems

We let the size of a game be the size of its arena, that is the number of positions. We study the complexity of the opacity problems.

First, note that Theorem 3 gives an EXPTIME upper bound to the opacity-guarantee problem: For an instance $A = (V, \Delta, \text{obs}, \text{act})$

and initial position v_0 of this problem, the safety game \widehat{A}_{v_0} of Theorem 3 can be solved in polynomial time. Indeed, as \widehat{A}_{v_0} is a perfect information game, it is determined, and the existence of a winning strategy for Geraldine can be decided by verifying whether her opponent, SuperRoberta, has a winning strategy. This amounts to solving a perfect information reachability game, and can be done in polynomial time [12], for example by a backward iteration from the target positions. Now, because the game \widehat{A}_{v_0} arises from a powerset construction, its size is exponential in the size of A . For the same reasons, thanks to Theorem 2, the opacity-violate problem also has an EXPTIME upper bound.

Still considering the opacity-violate problem, Proposition 2 provides a polynomial reduction of the D1-directing word problem, but cannot bring any tight lower bound, even if the D1-directing word problem would be proved PSPACE-complete.

To our knowledge, the exact complexity of the opacity-guarantee and opacity-violate problems are an open question.

However, in our attempt to develop efficient algorithms for the opacity-guarantee problem, we somehow rely on Theorem 3 and promote a top-down approach in the graph \widehat{A}_{v_0} . This approach should compete with the straightforward intractable bottom-up method to solve alternating reachability in \widehat{A}_{v_0} , that leads to the EXPTIME algorithm.

4 Towards a search-based algorithm

In this section we present the idea of an algorithm that, given a game with opacity-condition $A = (V, \Delta, \text{obs}, \text{act})$ over Σ and Γ , with v_0 as initial position, decides the existence of a winning strategy for Gerald and returns one if it exists.

The algorithm is based on a search approach in the graph of the perfect-information game \widehat{A}_{v_0} from Theorem 3. We distinguish between nodes in which it is SuperRoberta's turn to play and those in which it is Geraldine's. The first ones correspond to positions of the form (I, v) in \widehat{A}_{v_0} , the second ones to positions of the form

(I, v, a) . Since we want the computed strategy to be winning whatever SuperRoberta does, we have to provide a solution in all sons of SuperRoberta's nodes, entailing an AND-node interpretation of SuperRoberta's nodes. Dually in a Geraldine's node, it is sufficient to provide a solution for one of its sons to have a winning strategy, hence the OR-node interpretation of Geraldine's nodes. General search algorithms with heuristics on AND-OR graphs have already been studied [7, 8], but our setting is more involved. The halting condition of the search is subtle because we consider safety conditions in graphs that may contain cycles.

Halting conditions: There are only three ways to stop the exploration of a branch. The current node is:

- A losing position, thus this branch is cut.
- An OR-node (a Geraldine position) for which a safe strategy has already been found.
- An OR-node whose associated position is also associated to an ancestor.

The third point needs some justification. Assume we find an OR-node n' with an ancestor n both associated to position (I, v, a) . Two cases can be distinguished.

- The choice made at node n is not part of a winning strategy. If we expand the node n' , we have to be coherent with the strategy currently being constructed, thus the subtree rooted at n' is the same as the one rooted at n . It implies that the choice made at n can be proved wrong without expanding n' .
- The choice made at node n is part of a winning strategy. In this case n' doesn't need to be expanded neither since a solution has already been defined for the corresponding position, and exploring the rest of the subtree rooted at n will prove this choice correct.

Pruning: In this section we describe how we prune some branches during the search.

In an OR-node n , before expanding a son n' associated to position (I', v') , we check a sufficient condition for n' to be a position from which there is no winning strategy for Geraldine. This condition is that there exists a sequence of actions $a_1 \dots a_n$ that, if played by SuperRoberta from n' , will lead to a losing position whatever Geraldine does. This can be rephrased as a generalized D1-directing word problem in the non-deterministic automaton $\mathcal{A}_A = (V, \Sigma, \Delta')$, where transitions are added in order to obtain a complete automaton:

$$\Delta'(v, a) = \begin{cases} \Delta(v, a) & \text{if non-empty,} \\ \{\perp\} & \text{else.} \end{cases}$$

The problem becomes: does there exist a directing word w to a singleton different from $\{\perp\}$? Depth-first search techniques seem appropriate, and due to efficiency purposes, we may limit the length of the directing word by some parameter k_1 .

Heuristics: In OR-nodes, we use heuristics to order the expansion of unpruned sons. To compute the values assigned to these sons, we seek synchronizing words of minimal length in a deterministic automaton that, unlike \mathcal{A}_A , does not abstract Geraldine's moves. A synchronizing word w of length at most k_2 (a parameter) in this automaton reveals a winning play for SuperRoberta. The heuristics is that the longer the minimal synchronizing word, the more chances to avoid the singleton position. We can use breadth-first search techniques to compute minimal length directing words, no longer than k_2 .

5 Conclusion and perspectives

We have defined and studied in detail games with opacity condition, which address theoretical questions related to security aspects of computer systems. In order to bypass the intractable powerset-based procedure, we have proposed to exploit synchronizing words techniques from automata theory as heuristics for a top-down search algorithm.

We are currently developing this algorithm, with the pruning condition. Also, the proposed heuristics arises from an intuitive argument that deserves being validated in practice (by tuning parameters k_1 and k_2), and next theoretically justified.

Acknowledgement. We are very grateful to Dietmar Berwanger for initial discussions on this topic.

References

1. Dietmar Berwanger and Laurent Doyen. On the power of imperfect information. In R. Hariharan, M. Mukund, and V. Vinay, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, Dagstuhl, Germany, 2008. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.
2. Ján Černý. Poznámka k homogénnym experimentom s konečnými automatmi. *Mat. fyz. čas SAV*, 14:208–215, 1964.
3. Ján Černý, Alica Pirická, and Blanka Rosenauerova. On directable automata. *Kybernetika*, 7:289–298, 1971.
4. Krishnendu Chatterjee and Thomas A. Henzinger. Semiperfect-information games. In Ramaswamy Ramanujam and Sandeep Sen, editors, *FSTTCS*, volume 3821 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2005.
5. J. Dubreil, Ph. Darondeau, and H. Marchand. Opacity enforcing control synthesis. In *Workshop on Discrete Event Systems*, Gothenburg, Sweden, March 2008.
6. Imreh and Steinby. Directable nondeterministic automata. *ACTACYB: Acta Cybernetica*, 14, 1999.
7. V. Kumar and D. S. Nau. A general branch-and-bound formulation for and/or graph and game tree search. *Search in Artificial Intelligence*, pages 91–130, 1988.
8. A. Mahanti and A. Bagchi. AND/OR graph heuristic search methods. *Journal of the ACM (JACM)*, 32(1):28–51, 1985.
9. D. Martin. Borel determinacy. *Annales of Mathematics*, 102:363–371, 1975.
10. J-E Pin. Le problème de la synchronisation et la conjecture de černý. In A. De luca, editor, *Non-commutative structures in algebra and geometric combinatorics*, volume 109 of *Quaderni de la Ricerca Scientifica*, pages 37–48. CNR, Roma, 1981.
11. J-E Pin. On two combinatorial problems arising from automata theory. *Annals of Discrete Mathematics*, 17:535–548, 1983.
12. Reif. The complexity of two-player games of incomplete information. *JCSS: Journal of Computer and System Sciences*, 29, 1984.
13. A. Saboori and C.N. Hadjicostis. Opacity-enforcing supervisory strategies for secure discrete event systems. In *IEEE Conference on Decision and Control (CDC)*, Cancun Mexico, dec 2008.
14. Walter J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *J. Comput. System. Sci.*, 4:177–192, 1970.